PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :		(11) International Publication Number:	WO 92/07436
H04K 1/00	A1	(43) International Publication Date:	30 April 1992 (30.04.92)

(21) International Application Number: PCT/US91/03034

(22) International Filing Date: 30 April 1991 (30.04.91)

(30) Priority data:

597,784	19 October 1990 (19.10.90)	US
670,705	18 March 1991 (18.03.91)	US

(71) Applicant: SECURITY DYNAMICS TECHNOLOGIES, INC. [US/US]; One Alewife Center, Cambridge, MA 02140-2312 (US).

(72) Inventor: WEISS, Kenneth, P. ; 7 Park Avenue, Newton, MA 02159 (US).

(74) Agent: OLIVERIO, M., Lawrence; Wolf, Greenfield & Sacks, Federal Reserve Plaza, 600 Atlantic Avenue, Boston, MA 02210 (US).

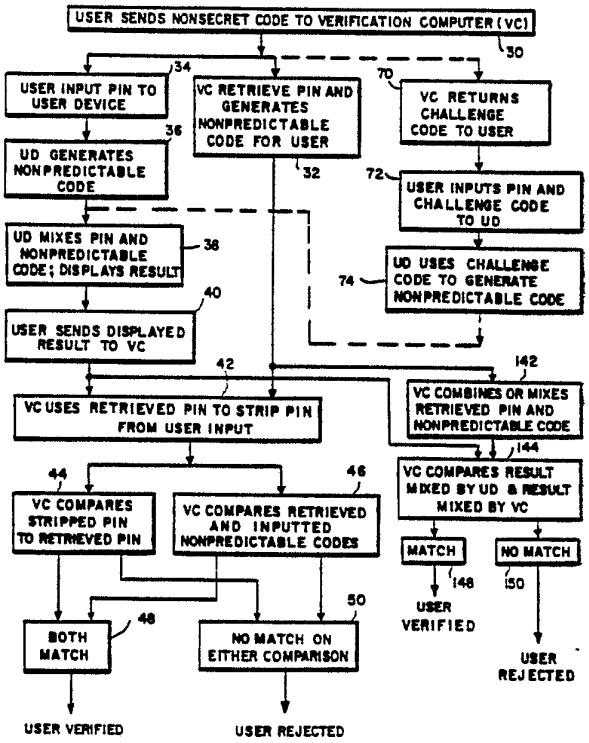
(81) Designated States: AT (European patent), AU, BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent).

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION

(57) Abstract

A method and apparatus for providing improved security for a personal identification number (PIN) in a personal identification and verification system of the type wherein a time dependent nonpredictable code is generated at a device in the possession of the individual (36), which code is unique to the individual and this code is communicated to, and compared with a nonpredictable code generated at a central verification computer (46). In this system, the PIN is mixed with the nonpredictable code before transmission of these values to the central verification computer (38). A nonsecret code (30) is previously transmitted to the central verification computer and is used by the verification computer to retrieve the PIN and independently generate the time dependent appropriate nonpredictable code for the user (74). These retrieved PIN and generated code values are used by the verification computer either (a) to strip the PIN from the transmitted nonpredictable code (42) and the stripped PIN and remaining nonpredictable code are compared with the corresponding retrieved values in order to determine verification (44, 46); or (b) to be mixed and then compared with the mixed PIN and code which is transmitted to the verification computer (144).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**ES**	Spain	**MG**	Madagascar
AU	Australia	**FI**	Finland	**ML**	Mali
BB	Barbados	**FR**	France	**MN**	Mongolia
BE	Belgium	**GA**	Gabon	**MR**	Mauritania
BF	Burkina Faso	**GB**	United Kingdom	**MW**	Malawi
BG	Bulgaria	**GN**	Guinea	**NL**	Netherlands
BJ	Benin	**GR**	Greece	**NO**	Norway
BR	Brazil	**HU**	Hungary	**PL**	Poland
CA	Canada	**IT**	Italy	**RO**	Romania
CF	Central African Republic	**JP**	Japan	**SD**	Sudan
CG	Congo	**KP**	Democratic People's Republic of Korea	**SE**	Sweden
CH	Switzerland			**SN**	Senegal
CI	Côte d'Ivoire	**KR**	Republic of Korea	**SU**+	Soviet Union
CM	Cameroon	**LI**	Liechtenstein	**TD**	Chad
CS	Czechoslovakia	**LK**	Sri Lanka	**TG**	Togo
DE*	Germany	**LU**	Luxembourg	**US**	United States of America
DK	Denmark	**MC**	Monaco		

+ Any designation of "SU" has effect in the Russian Federation. It is not yet known whether any such designation has effect in other States of the former Soviet Union.

METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION

Cross Reference to Other Applications

This application is a continuation-in-part of application serial no. 07/341,932 filed April 21, 1989, which is a continuation-in-part of application serial no. 802,579 filed November 27, 1985, issued December 5, 1989 as U.S. Patent No. 4,885,778, which application is itself a continuation-in-part of application serial no. 676,626 filed November 30, 1984, now U.S. Patent No. 4,720,860, issued January 19, 1988. The disclosures and specifications of all of the foregoing applications/patents are incorporated herein by reference as if fully set forth.

Field of the Invention

This invention relates to methods and apparatus for identifying an individual and more particularly to methods and apparatus for providing improved security for a personal identification number (PIN) utilized in conjunction with such an identification system.

Background of the Invention

Personal identification systems may be based on something someone has, such as a card or badge, something that someone knows, such as a PIN, or some characteristic of the individual, such as his fingerprints or speech pattern. Security for such systems is enhanced by utilizing two or more of the above in performing the identification.

For example, parent Patent No. 4,720,860, discloses a personal identification system wherein the individual has a card or other small, portable device which contains a microprocessor programmed to utilize a secret algorithm to generate a nonpredictable number from a stored value unique to the individual and a time varying value provided for example by a clock. The nonpredictable value is preferably displayed on the device. The individual then enters his secret PIN into a central verification system, either directly or over a telephone line, causing the central system to access

stored information corresponding to the individual and to utilize at least some of this information to generate a nonpredictable value at the central computer utilizing the same algorithm as at the individual's microprocessor. At the same time this is being done, the individual is entering the number appearing at that period of time on the display of his device. The two values will match, signifying identification of the individual, only if the individual has entered the correct PIN and if the individual has the proper device so that the nonpredictable code displayed corresponds to that being generated at the central verification computer.

In other systems, such as those shown in U.S. Patent No. 4,599,489 issued July 8, 1986, the PIN may either be stored in the user's device, or may be entered by the user. If the PIN is stored in the device, it is read from the device by a suitable reader and causes the central verification computer to generate a unique challenge code to the individual. This challenge code may either be entered by the individual into his machine, or may be automatically sensed by the machine, and is operated on by the user's device to generate a unique nonpredictable code which is then entered into the central computer to effect verification.

One potential difficulty with either of the systems indicated above is that an unauthorized

individual may be able to obtain access to the user's PIN by electronic eavesdropping, reducing the security provided by the system. If, for example, the PIN is transmitted over public lines, such as telephone lines, from the user to the central verification computer, it may be possible to tap these lines and intercept the PIN as it is being transmitted. If the PIN is stored in the device, someone obtaining the device surreptitiously may, through sophisticated means, be able to determine the PIN stored in the device and thus defeat the security of the system. Furthermore, any storing of a PIN or password in the portable device for comparison defeats the purpose of an independent identification factor and reduces security to a "thing" possessed.

A need therefore exists for an improved means of communicating a PIN or other user identification code to a central verification system such that someone tapping the line over which the code is being sent will be unable to determine the secret identification number and someone obtaining possession of the user device will also not be able to obtain access to the user's secret identification number from the device.

Summary of the Invention

In accordance with the above, this invention provides a method for personal identification and apparatus for the practice thereof wherein a device in the possession of the individual is utilized to generate a unique, time varying, nonpredictable code; the nonpredictable code generated at a given time is mixed with a secret PIN for the individual; the mixed output is communicated to a central verification computer; and the verification computer typically strips the PIN from the communicated value and utilizes the stripped PIN and remaining nonpredictable code to perform a verification operation. Alternatively and equivalently, the mixed output which is communicated to the verification computer may be verified in the verification computer without stripping of the PIN. Preferably, before the mixed value is communicated to the verification computer, a nonsecret identifying code for the individual is communicated to the verification computer; the verification computer utilizes the nonsecret identifying code to obtain the PIN and appropriate nonpredictable code for the individual; and the verification operation includes the PIN and appropriate nonpredictable code obtained during the obtaining step being compared with the stripped PIN and remaining nonpredictable code. Alternatively the PIN may not be stripped

from the mixed value, the verification computer may utilize the nonsecret identifying code to retrieve or obtain the PIN and appropriate nonpredictable code, combine the retrieved PIN and appropriate nonpredictable code, and perform a verification operation between the mixed value communicated to the verification computer and the combination of the retrieved PIN and appropriate nonpredictable code. The verification computer may also generate a unique challenge value in response to the nonsecret identifying code which challenge code is communicated to the device in possession of the individual. For one embodiment, the challenge code is communicated to the individual and the individual inputs the challenge value and the PIN to his device, the device includes means responsive to the challenge value for generating the nonpredictable code. During the mixing step, the device may receive the PIN and the nonpredictable code and generate an output which is a predetermined function of the inputs. The predetermined function may, for example, be a sum of the inputs, for example the sum of the inputs without carry.

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention as illustrated in the accompanying drawings.

In the Drawings

Fig. 1 is a semi-block schematic diagram of the verification system of a first embodiment of the invention.

Fig. 2 is a block schematic diagram of a second embodiment of the invention.

Fig. 3 is a block flow diagram illustrating the operation of the first embodiment of the invention and alternative steps for the second embodiment of the invention.

Detailed Description

Fig. 1 shows illustrative structure for a personal identification system of a first embodiment of the invention. In this figure, a user verification device 10 is provided which is of the type described in the parent applications. The device is preferably of the general size and shape of a standard credit card, although its thickness dimension may be slightly greater than that of such cards. The device 10 has a clock which generates a time-dependent digital output to a microprocessor which is programmed with a unique algorithm to operate on the time-dependent clock input and on a stored static value unique to a given user to generate a multi-bit nonpredictable code. A plurality of input areas 12 are provided on the face of device 10. These areas are preferably each

indicative of a numerical digit, for example the digits 1 - 0 as shown in Fig. 1, and may be pressure-sensitive pads or otherwise adapted to generate an electrical output indicative of the area when the area is touched by the user. Spacing may be provided between the individual areas 12 to assure distinctive outputs. As will be described in greater detail hereinafter, the user may input his unique PIN on areas 12 which are mixed in the processor in device 10 with the nonpredictable code generated therein in response to the time-dependent and static inputs to generate a multi-bit nonpredictable code which is displayed on area 14 of device 10. Area 14 may be a liquid crystal display or other suitable display device for producing numeric or alpha-numeric characters. Each area of display 14 is adapted to display a different digit of the nonpredictable code.

The user initially transmits a nonsecret identifying code to verification computer 16 by keying this number into a telephone 18 at his location. This number is transmitted over telephone lines 20 to telephone 22 at the verification station and through a modem 24 at this station to the verification computer. The user may then use the telephone 18 to key in and transmit the nonpredictable code being displayed at that time on display 14.

Fig. 3 is a flow diagram illustrating in greater detail the operation of the system of Fig. 1 to perform a verification operation. Referring to Fig. 3, the first step in the operation, step 30, is for the user to send his nonsecret code to verification computer (VC) 16. As previously indicated, this is accomplished by the user keying his nonsecret identification number into telephone 18 for transmission through telephone line 20, telephone 22 and modem 24 to the verification computer.

In response to the user input of his nonsecret code, the verification computer retrieves the user's PIN and generates the nonpredictable code for the user, using the same algorithm and stored static value as user device 10, and using a time-related value from a clock device at the verification computer, which is maintained in synchronism with the clock at the user device in a manner discussed in the parent application (step 32). At the same time that the verification computer is retrieving the PIN and nonpredictable code for the user, the user is inputting his PIN into his device 10 using key pads or areas 12 (step 34). While the user is inputting his pin, the user device is continuously generating nonpredictable code values at its internal processor in response to the clock value and the stored static value using the unique algorithm at the user device processor (step 36).

The next step in the operation, step 38, is for the generated nonpredictable code and the inputted pin to be mixed by the processor in device 10 to generate a new nonpredictable code which is displayed on display 14. The mixing operation may be a simple addition of the two values without carry, or with carry, (a constant added to a pseudo random number produces a pseudo random number) or may involve a more sophisticated mixing algorithm.

During step 40, the user transmits the displayed value by use of telephone 18 through telephone line 20, telephone 22, and modem 24 to verification computer 16.

During the next step in the operation, step 42, the verification computer uses the PIN for the user which was retrieved during step 32 to strip the PIN from the inputted nonpredictable code, the result being a PIN value and a nonpredictable code value. During step 44 the stripped PIN is compared with the PIN retrieved during step 32 and during step 46 the nonpredictable code remaining after the inputted value has the PIN stripped therefrom is compared with the retrieved nonpredictable code. If matches are obtained during both steps 44 and 46 (step 48) the verification computer signifies verification. If a match is not found during either step 44 or step 46 (step 50) then the user is rejected.

Alternatively to steps 42, 44, 46, 48 and 50, the PIN and nonpredictable code which are retrieved in step 32 may be combined or mixed by the verification computer during step 142 according to the same mixing operation which was carried out by the processor or user device 10 in step 38, e.g. by a simple addition of the two values without carry, with carry, or according to some other more sophisticated algorithm. During alternative step 144 the separate results of the mixing operations carried out by the user device 10 and the verification computer 16 are compared. If a match is obtained, step 148, the user is verified. If a match is not found, step 150, the user is rejected.

A procedure is thus provided wherein user verification may be obtained using the simple and inexpensive procedure disclosed in the parent applications while still providing a high level of security for the user PIN. This security is achieved since the user PIN is never available on an open line which could be tapped except in the form of a word which is a mixture of the PIN with a nonpredictable code and which is virtually impossible to decipher.

Fig. 2 illustrates an alternative configuration in which the teachings of this invention may be utilized. In Fig. 2, the user device 10 is of the same type shown in Fig. 1. However, for this

embodiment of the invention, the user device is adapted to be used in proximity to the verification station rather than from a remote location over telephone lines. For this embodiment of the invention, the verification station 60 includes a computer 62, a display 64, such as for example a CRT display, and an input device 66 which may, for example, be a standard computer input keyboard. Referring again to Fig. 3, the operation with this embodiment of the invention starts with step 30, during which the user sends a nonsecret code to the verification computer 62 by, for example, keying this code into input device 66. In response to receiving the nonsecret code, computer 60 retrieves the PIN and generates the nonpredictable code for the user (step 32) and also retrieves a challenge code for the user which is displayed on display 64 (step 70). The user inputs his PIN and the challenge code in an order established for the system to user device 10 using input pads 12 (step 72). During step 74, the processor in device 10 uses the inputted challenge code and the time inputted from its clock to generate a nonpredictable code which, during step 38, is mixed with the inputted pin and the results are displayed on display 14 of device 10. From this point on, the operation for this embodiment of the invention is the same as that previously described with respect to the embodiment of Fig. 1.

Thus, with this embodiment of the invention, as with the prior embodiment of the invention, the pin in uncoded form is never transmitted in a manner such that it could be observed and is not resident in the user's device where it might, using sophisticated technology, be retrieved.

As an alternative to the embodiment shown in Fig. 2, the nonsecret code may be recorded in machine-readable form on device 10 and input device 66 might include a card reader which the card is inserted into to permit the nonsecret code to be read into computer 62.

While the invention has been shown and described above with reference to preferred embodiments, the foregoing and other changes in form and detail may be made therein by one skilled in the art without departing from the spirit and scope of the invention.

What is claimed is:

CLAIMS

1. In a personal identification system of the type wherein a user is provided with a device generating a unique, time-varying, nonpredictable code, with a nonsecret identifying code and with a secret PIN, the nonpredictable code at a given instant and the PIN being provided to a central verification computer to effect verification; apparatus for providing improved security for the PIN comprising:

means for mixing the nonpredictable code generated by the device at a given time with the PIN according to a predetermined algorithm to generate a combined coded value;

means for separately communicating the nonsecret identifying code and the combined coded value to the central verification computer; and

wherein the central verification computer includes means for utilizing the nonsecret identifying code to retrieve the PIN and generate an appropriate, unique, time varying nonpredictable code for the individual, and at least one of:

(a) a means for utilizing the retrieved PIN, appropriate nonpredictable code and the combined coded value in performing a verification operation; or

(b) a means for stripping the PIN from the combined coded value received from the means for communicating, the nonpredictable code remaining after stripping of the PIN and means for utilizing the retrieved PIN, and appropriate nonpredictable code for performing a verification operation.

2. Apparatus as claimed in claim 1 including means operative prior to the communicating of the value from the mixing means for communicating the nonsecret identifying code to said verification computer.

3. Apparatus as claimed in claim 2 wherein said verification computer includes means for utilizing the communicated nonsecret identifying code to retrieve the PIN and a unique challenge value for the individual; and

means for communicating the challenge value to the device.

4. Apparatus as claimed in claim 3 wherein said challenge value communicating means includes means for communicating the challenge value to the individual; and

wherein the device includes means for permitting the individual to input the challenge value and his PIN to the device.

5. Apparatus as claimed in claim 4 wherein said device includes means responsive to the challenge value for generating the nonpredictable code; and

wherein said mixing means includes means, included as part of the device, for receiving the inputted PIN and the generated nonpredictable value and for generating an output which is a predetermined function of the input.

6. Apparatus as claimed in claim 5 wherein said mixing means adds the PIN to the nonpredictable code.

7. Apparatus as claimed in claim 1 wherein said device includes means for permitting the individual to input his PIN to the device; and

wherein said means for mixing is included as part of said device and is adapted to receive the PIN inputted by the individual and the nonpredictable code and to generate an output which is a predetermined function of the input.

8. Apparatus as claimed in claim 7 wherein said mixing means adds the PIN to the nonpredictable code.

9. Apparatus as claimed in claim 1 wherein said verification computer includes a means for mixing the retrieved PIN and appropriate nonpredictable code generated by the verification computer at a given time according to the predetermined algorithm to generate a second combined coded value.

10. Apparatus as claimed in claim 9 wherein the verification operation comprises comparing the combined coded value with the second combined coded value.

11. Apparatus as claimed in claim 1 wherein the means for performing a verification operation includes means for comparing the PIN and nonpredictable code obtained in response to the nonsecret identifying code with the stripped PIN and remaining nonpredictable code.

12. A method for identifying an individual comprising the steps of:

utilizing a device in the possession of the individual to generate a unique time-varying, nonpredictable code;

mixing the nonpredictable code generated at a given time with a secret PIN for the individual to generate a combined code; and

communicating a nonsecret identifying code for the individual and the combined code to a central verification computer;

the verification computer utilizing the nonsecret identifying code to retrieve the PIN and generate an appropriate, unique, time-varying nonpredictable code for the individual, and at least one of:

(a) utilizing the retrieved PIN, appropriate nonpredictable code, and the combined code to perform a verification operation; or

(b) stripping the PIN from the communicated combined code and utilizing the retrieved PIN and nonpredictable code, the stripped PIN and the remaining nonpredictable code to perform a verification operation.

13. A method as claimed in claim 12 wherein the verification computer also generates a unique challenge value in response to the nonsecret identifying code; and

including the step of communicating the challenge value to the device in possession of the individual.

14. A method as claimed in claim 13 wherein the challenge value is communicated to the individual; and

including the step of the individual inputting the challenge value and his PIN to the device.

15. A method as claimed in claim 14 wherein the device includes means responsive to the challenge value for generating the nonpredictable code; and

wherein the mixing step includes the device receiving the PIN and the nonpredictable code and generating an output which is a predetermined function of the inputs.

16. A method as claimed in claim 15 wherein said predetermined function is a sum of said inputs.

17. A method as claimed in claim 15 including the step of the individual inputting his PIN to the device; and

wherein the mixing step includes the device receiving the PIN inputted by the individual and the nonpredictable code and generating an output which is a predetermined function of the inputs.

18. A method as claimed in claim 17 wherein said predetermined function is a sum of said input.

19. A method as claimed in claim 12 wherein the verification computer utilizes the retrieved PIN and

appropriate nonpredictable code by combining them to obtain a second combined code.

20. A method as claimed in claim 19 wherein the verification operation comprises comparing the combined code and the second combined code.

21. A method as claimed in claim 12 wherein the verification operation includes comparing the retrieved PIN and the nonpredictable code generated by the verification computer with the stripped PIN and the remaining nonpredictable code.

1/2

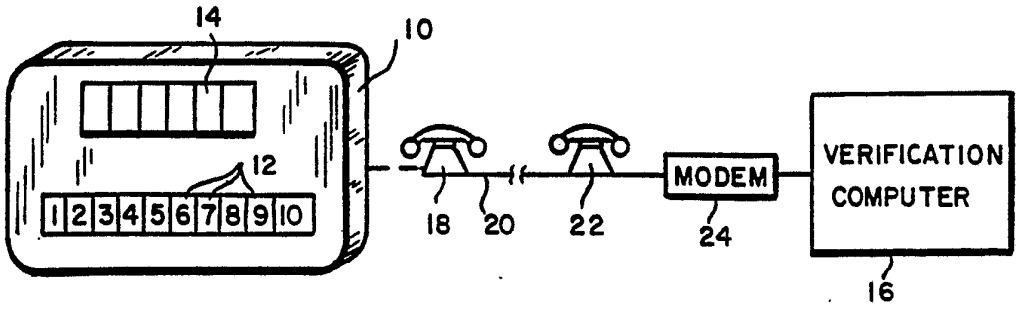

14
10
12
1 2 3 4 5 6 7 8 9 10
18
20
22
MODEM
24
VERIFICATION COMPUTER
16

FIG. 1

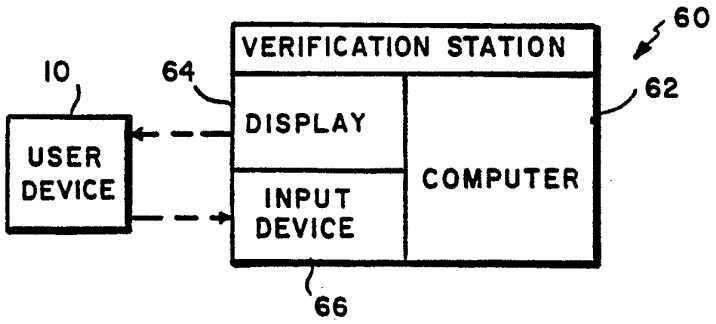

60
VERIFICATION STATION
10
64
62
USER DEVICE
DISPLAY
INPUT DEVICE
COMPUTER
66

FIG. 2

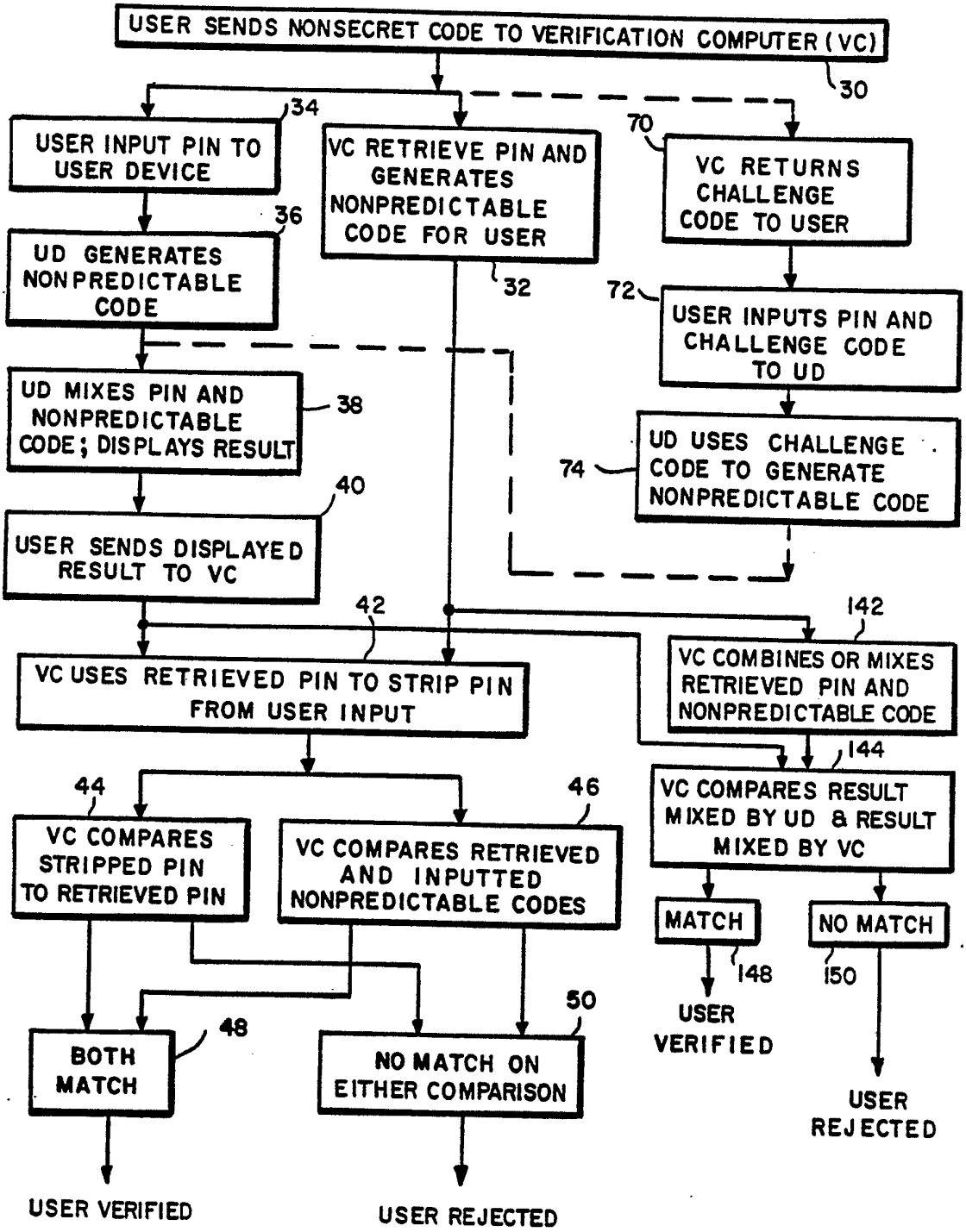

USER SENDS NONSECRET CODE TO VERIFICATION COMPUTER (VC)
30
USER INPUT PIN TO USER DEVICE
34
VC RETRIEVE PIN AND GENERATES NONPREDICTABLE CODE FOR USER
32
VC RETURNS CHALLENGE CODE TO USER
70
UD GENERATES NONPREDICTABLE CODE
36
USER INPUTS PIN AND CHALLENGE CODE TO UD
72
UD MIXES PIN AND NONPREDICTABLE CODE; DISPLAYS RESULT
38
UD USES CHALLENGE CODE TO GENERATE NONPREDICTABLE CODE
74
USER SENDS DISPLAYED RESULT TO VC
40
VC USES RETRIEVED PIN TO STRIP PIN FROM USER INPUT
42
VC COMBINES OR MIXES RETRIEVED PIN AND NONPREDICTABLE CODE
142
VC COMPARES RESULT MIXED BY UD & RESULT MIXED BY VC
144
VC COMPARES STRIPPED PIN TO RETRIEVED PIN
44
VC COMPARES RETRIEVED AND INPUTTED NONPREDICTABLE CODES
46
MATCH
148
NO MATCH
150
USER VERIFIED
BOTH MATCH
48
NO MATCH ON EITHER COMPARISON
50
USER REJECTED
USER VERIFIED
USER REJECTED

FIG.3

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US91/03034

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC(5) H04K 1/00
US 380/23,25

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
US	380/23,24,25,28,48

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category *	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
X	US,A 4,720,860 (WEISS) 19 January 1988	1-21
A	US,A 4,890,323 (BEKER ET AL) 26 December 1989	1-21
A	US,A 4,885,778 (WEISS) 05 December 1989	1-21
A	US,A 4,856,062 (WEISS) 08 August 1989	1-21
A	US,A 4,819,267 (CARGILE ET AL) 04 April 1989	1-21
A	US,A 4,802,216 (IRWIN ET AL) 31 January 1989	1-21
A	US,A 4,731,841 (ROSEN ET AL) 15 March 1988	1-21
A	US,A 4,599,489 (CARGILE) 08 July 1986	1-21
A	US,A 4,578,530 (ZEIDLER) 25 March 1986	1-21
A	US,A 4,509,093 (STELLBERGER) 02 April 1985	1-21

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
21 August 1991	27 SEP 1991
International Searching Authority	**Signature of Authorized Officer**
ISA/US	For David Cain — NGUYEN NGOC-HO, INTERNATIONAL DIVISION

Form PCT/ISA/210 (second sheet) (Rev.11-87)